DEPARTMENT OF THE ARMY
OFFICE OF THE PROGRAM EXECUTIVE OFFICER
ENTERPRISE INFORMATION SYSTEMS
(PEO EIS)
9350 HALL ROAD, SUITE 141
FORT BELVOIR, VIRGINIA 22060-5526

REPLY TO
ATTENTION OF

SFAE-PS

15 April 2005

MEMORANDUM FOR: PM, Transportation Information Systems (TIS), ATTN: SFAE PS-TC, 8000 Corporate Court, Springfield, VA 22153

SUBJECT: Approval to Operate (ATO) for the Product Manager Transportation Information System (PM TIS) Enterprise Management System (EMS)

1. References:

a. DoDI 5200.40, 30 December 1997, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)

b. DoDI 8500.2, 6 February 2003, Information Assurance (IA) Implementation

c. AR 25-2, 14 November 2003, Information Assurance

d. Memo AMSEL-IE-IA, 26 Jan 04, Subject: TIS Enterprise and Transportation Coordinators' Automated Information for Movements System II (TC-AIMS II) Accreditation Recommendation and Clarification

e. Memorandum SFAE-PS-TC, 31 March 2005, Subject: Request Extension of Approvals to Operate (ATO) the Transportation Information Systems (TIS) Central Management Facility (CMF) and the Transportation Coordinators' Automated Information for Movements System II (TC-AIMS II)

2. The TIS Enterprise currently hosts Transportation Information Systems – Theater Operations (TIS-TO) (formerly known as Department of the Army Movements Management System Re-design (DAMMS-R) Block III) and TC-AIMS II. The TIS Enterprise is protected by a perimeter router, perimeter and internal firewalls, enterprise anti-virus software and an IDS system. User access to the Enterprise is restricted by IP address and limited to ".mil" addresses only. Users are directed to a secure web page requiring authentication using valid TIS credentials. These credentials are used to communicate through an integrated Citrix Service, to obtain a list of applications the user is authorized access. All access is restricted and controlled through this CITRIX front-end.

3. A security survey was conducted of the TIS Enterprise Management System (EMS) in April 2005, where system capabilities and management processes were evaluated by the Infortmation Assurance Security Engineering Directorate (IASED), Information Systems Engineering Command (ISEC), Certification Authority (CA) for this platform. It was determined that many of the TIS EMS procedures are still maturing. It was also determined that the TIS EMS is well protected from outside threats by an extensive defense-in-depth strategy.

4. I have reviewed the results of the security testing and with consideration of the risk mitigation strategy provided, the overall system risk is evaluated as MODERATE. I concur with the findings of

moderate for the TIS EMS. This risk has been weighed against the operational requirements and security measures that have or will be implemented in the area of physical, personnel, hardware, software, procedural, and communications security. Approval of this request for an Approval to Operate (ATO) is in the best interest of the government.

5. The PM TIS is currently enhancing the security posture of all TIS applications by migrating them to the TIS EMS environment. The TIS EMS will host additional applications to include but not be limited to: Automated Air Load Planning System (AALPS), Deployment and Sustainment Support Tool (DS2T), and Automated Movement Flow Tracking – Command Information System (AMFT-CIS). As such it is the responsibility of the PM Transportation Information Systems (PM TIS) to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or any other modification is reported to my point of contact for this action and is analyzed to determine its impact on sysetm security. Additionally I attach the following provisions to this Approval to Operate:

- the TIS EMS security and accreditation documentation is still evolving, and must be updated as additional detailed information is made available to accurately and thoroughly document the operational system aspects of the security processes and procedures. The System Security Authorization Agreement, Security Concept of Operations, IAVM Compliance, and other system artifacts must maintain detailed system, interface, and operational information. This documentation must be kept current as the system matures to provide the most accurate information possible to system users and administrators.

- the Plan of Action and Milestones (PoA&M) must be kept current until all known and documeted risks have been mitigated to an acceptable level or a waiver obtained from compliance. Monthly reviews will be conducted by PM TIS with the results forwarded to my point of contact.

- an Information Assurance (IA) Integrated Product Team (IPT) must be established to develop security mitigation strategies and ensure compliance with all applicable IA controls. The IPT at a minimum will meet monthly and include, representatives from the PM TIS security engineering team, the Certification Authority, and the PEO EIS Office of Information Assurance and Compliance (OIA&C).

6. Accordingly, by authority delegated to me, an Approval to Operate (ATO) for the PM Transportation Information System (PM TIS) Enterprise Management System (EMS) is granted for a period of 12 months from the date of this letter.

7. My point of contact for this action is Lawrence M. Coclough, Senior Information Assurance Official (SIAO), (703) 806-3388,DSN 656.

KEVIN CARROLL
Program Executive Officer